IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
	*	
v.	*	**CRIMINAL NO. LKG-25-6**
	*	
THOMAS C. GOLDSTEIN,	*	
	*	
Defendant	*	
	*	

****

GOVERNMENT'S OPPOSITION TO DEFENDANT'S
APPEAL OF AMENDED CONDITIONS OF RELEASE

The United States of America respectfully requests that the Court deny Defendant's Appeal of Amended Conditions of Release, ECF 81. Chief Magistrate Judge Sullivan correctly ordered monitoring of the Defendant's electronic devices ("Monitoring Condition"). Defendant remains a significant flight risk and the Monitoring Condition is supported by (1) the Bail Reform Act factors; (2) Defendant's failure to disclose his assets, including cryptocurrency, to the Government and the Court; and (3) Defendant's recent, substantial use of cryptocurrency and efforts to conceal that use, as well as ongoing criminal conduct. Accordingly, the Court should affirm Defendant's Amended Order on Conditions of Release.

BACKGROUND

On January 16, 2025, a federal grand jury returned a twenty-two count Indictment against Defendant for violations of federal tax laws and for making false statements on mortgage loan applications. ECF 1. On January 27, 2025, Defendant made his initial appearance before Judge Sullivan and pleaded not guilty to all the charges. ECF 4. Defendant was released on conditions, including a requirement that Defendant execute a bond for 100% interest in his residence in Washington, D.C. ECF 6 at 2.

On January 29, 2025, Defendant filed a motion to modify the forfeiture bond by substituting three South Carolina properties for the Washington, D.C. residence. ECF 18. On January 29, 2025, Judge Sullivan denied the request to substitute the South Carolina properties for the Washington, D.C. residence because the use of the Washington, D.C. residence as security was "necessary to reasonably assure that Mr. Goldstein will appear for all future proceedings in this case." ECF 19 at 1. On February 5, 2025, Defendant filed a *pro se* appeal of that condition to the District Court. ECF 30.

On February 9, 2025, the Government filed an *ex parte* motion to revoke Defendant's conditions of release, alleging that Defendant had failed to disclose to his supervising Pretrial Services officer that he owned two cryptocurrency accounts and had failed to obtain approval from Pretrial Services before transferring funds from those accounts. ECF No. 35. On February 10, 2025, the Court granted the Government's motion and issued an arrest warrant for Defendant. ECF No. 37. The same day, Defendant was arrested at the courthouse and appeared before the Court. ECF No. 42. After hearing from the parties, Judge Sullivan entered an Order of Detention, finding that there was clear and convincing evidence that Defendant violated his conditions of release by (1) failing to disclose his ownership interest in two cryptocurrency accounts (the "935B" wallet and the "54E3" wallet), and (2) making transfers from those accounts without the permission of Pretrial Services. ECF 42; *see also* ECF 64 (Memorandum Opinion) at 2.

On February 11, 2025, Defendant filed a motion to revoke the order of detention. ECF 44. The Government filed a response the same day and Defendant filed a reply the next day. ECF 51, 54. Judge Sullivan held a hearing on February 13, 2025. At the conclusion of the hearing, Judge Sullivan ordered Defendant released on amended conditions, including the Monitoring Condition. ECF 61, 62.

Judge Sullivan also issued a Memorandum Opinion, explaining his decision. ECF 64. Judge Sullivan stated that after receiving encrypted messages proffered by Defendant, which were not previously available to the Government, the Court was no longer convinced by clear and convincing evidence that Defendant violated his conditions of release. *Id.* at 4. However, Judge Sullivan noted the Court was "highly suspicious" that Defendant used cryptocurrency while on conditions of release. *Id.* at 5. The Court explained:

> There is ample evidence that Mr. Goldstein has been and remains a sophisticated and frequent user of cryptocurrency for years. He has used cryptocurrency—or directed others to use it on his behalf—to pay for everything from gambling losses to luxury watches for multiple women. *See* ECF No. 52. And it now even appears that Mr. Goldstein currently has cryptocurrency accounts—besides the 935B and 54E3 wallets—that he controls, and of which he did not inform his supervising Pretrial Services officer.

Id. Based on these findings, Judge Sullivan observed that, "[i]f the preponderance of the evidence standard applied under 18 U.S.C. § 3148(b), Mr. Goldstein would remain detained." *Id*.

In addition to ordering Defendant's release, Judge Sullivan entered an order amending Defendant's conditions of release under 18 U.S.C. § 3142(c)(3), which provides that "[t]he judicial officer may at any time amend the order to impose additional or different conditions of release." ECF 62, 64 at 5–6. The amended conditions of release explicitly required Defendant to disclose to Pretrial Services all his assets, including cryptocurrency, prohibited Defendant from engaging in cryptocurrency transactions, and ordered monitoring of Defendant's internet capable devices by Pretrial Services. ECF 62 at 3. Judge Sullivan explained, "These added restrictions are necessary to reasonably assure that Mr. Goldstein appears as required. Given Mr. Goldstein's extensive past use of cryptocurrency, the Court finds it likely that Mr. Goldstein has access to funds that have yet to be identified, and which he might use to flee from prosecution in this case." ECF 64 at 6.

On February 14, 2025, this Court held a hearing and denied without prejudice Defendant's appeal to substitute the South Carolina properties for the Washington, D.C. residence. ECF 71, 72. The Court followed the hearing with a Memorandum Opinion. ECF 76.

On February 27, 2025, Defendant filed the instant appeal to the District Court regarding the Monitoring Condition imposed by Judge Sullivan. ECF 80. Under the Bail Reform Act, the Court reviews this condition of release *de novo*. *See* 18 U.S.C. § 3145(a); *United States v. Clark*, 865 F.2d 1433, 1436-38 (4th Cir. 1989); *United States v. Stewart*, 19 F. App'x 46, 48 (4th Cir. 2001).[1]

[1] Defendant spends much of his appeal attacking the Government and Judge Sullivan's order, rather than addressing the Bail Reform Act factors. The Court should not be persuaded by these baseless attacks, and the Government will not respond to them in detail. Three points, however, merit attention.

First, although Defendant was ordered released, Judge Sullivan found by a preponderance of evidence that Defendant engaged in prohibited cryptocurrency transactions while on release, and that the Government acted in good faith. *See* ECF 73 (Tr. of February 13, 2025 hearing) at 23.

Second, before Judge Sullivan and in the instant appeal, Defendant repeatedly asserts that the Government "misled" the Court. Not so. For example, during the February 13, 2025 hearing before Judge Sullivan, defense counsel repeatedly argued that the Government falsely claimed Defendant met with the Pretrial Services officer to review Defendant's financial accounts on February 6, 2025. *See* ECF 73 at 18–19 (Tr. of Feb. 13, 2025 hearing) (Mr. Kravis: "[W]e pointed to numerous misleading characterizations of evidence or just outright false statements that were made in the Government's *ex parte* motion . . . I'm just going to give the court one example, and that is, the Government's motion alleged that on February 6th Mr. Goldstein had an in-person meeting with pretrial services where he was asked about all of his accounts and he did not mention the cryptocurrency accounts. *That meeting did not happen*." (emphasis added)).

But, contrary to counsel's representations, that meeting did, in fact, happen—as Pretrial Officer Smith confirmed during the hearing. *See Id.* at 27 (Mr. Smith: "So I'll start with the February 6th appointment. It was an appointment that happened virtually. And in that appointment we did go over the accounts, the financial accounts information that he had provided to me via text … It was by FaceTime." The Court: "So your position is that Mr. Goldstein's proffer to me was incorrect because you did have the meeting?" Mr. Smith: "That is correct."). While the Government is sure that this was an honest mistake by defense counsel, it demonstrates why the Court should disregard Defendant's renewed accusations made on appeal.

Third, Defendant now states that the Government did not provide to the Court evidence that defense counsel (who did not represent Defendant at the time) proffered to the Government after the February 10 detention hearing. *See* ECF 81 at 6. This is also false. At that detention hearing, Defendant elected, after a *Faretta* hearing, to proceed *pro se*. *See* ECF 69 (Tr. of Feb. 10, 2025 hearing) at 4–16. Thus, Defendant was no longer represented by counsel. That evening, former counsel emailed the Government with two

ARGUMENT

Judge Sullivan was correct to order the monitoring of Defendant's electronic devices as part of Defendant's conditions of release. Defendant's appeal does not justify reversing that decision. Notably, Defendant's motion does not address the applicable factors under 18 U.S.C. § 3142 that the Court "shall" consider in determining what conditions of release are appropriate. *See* 18 U.S.C. § 3142(g).[2] Those factors make clear that the Monitoring Condition is necessary to "reasonably assure the appearance of [Defendant] as required and the safety of any other person and the community." *Id.*

I. Bail Reform Act Factors

a. Nature and Circumstances of Offense

As this Court found when denying without prejudice Defendant's previous appeal of his release conditions, "the offenses charged in this case are quite serious" and "the nature and circumstances of the offenses alleged in this case weigh in favor of imposing conditions of release that will mitigate the Defendant's serious risk of flight." ECF No. 76 at 5, 6. Defendant's "serious

encrypted message threads—which the Government did not previously have—about the 2023 transfers to the 935B and 54E3 wallets. Even though the Government was under no obligation to do so, the Government emailed the messages to Judge Sullivan's chambers *ex parte*, recognizing that Defendant was representing himself *pro se* and was detained. The Government later referenced this during the February 13 hearing. *See* ECF 73 at 20 (Mr. Kibbe: I also have a copy of the [separate February 11] transfers right here for the Court if you would like to see them and was planning on bringing them to the court's attention, *just like we brought the other evidence to the court's attention*." (emphasis added)). Defendant's overblown rhetoric distracts from the Bail Reform Act and the evidence, which demonstrate that the Court should affirm the current conditions of release.

[2] Neither the Defendant nor the Government is appealing Judge Sullivan's finding that there was a preponderance of evidence, but not clear and convincing evidence, that Defendant violated his conditions of release by transferring funds using the "935B" and "54E3" wallets. Therefore the question is *not* whether the Government proved by clear and convincing evidence that Defendant exclusively controlled those wallets. Rather, the amended conditions of release were imposed under 18 U.S.C. § 3142(c)(3) based on all the information before the Court, and therefore the standard Bail Reform Act analysis applies.

risk of flight" has not changed in the three weeks since the Court's previous order, and the nature and circumstances of the offense weigh in favor of the Monitoring Condition.

i. The Charges

As relevant to the Monitoring Condition, Defendant has been charged with twenty-two counts of tax crimes and making false statements to mortgage lenders. At the core of this conduct, Defendant repeatedly hid his assets and lied to or otherwise mislead the federal government and private parties. Defendant is charged with hiding millions of dollars in income from the IRS. Defendant is also charged with lying to an IRS Revenue Officer about the source of his income. Defendant is further charged with making patently false statements to mortgage lenders on three different mortgage applications to benefit himself in purchasing a new multi-million-dollar residence, ECF 1 ¶¶ 89-94, 97-100.

ii. Defendant's International Travel and Contacts

Defendant's crimes were inextricably intertwined with international travel and contacts. For example, Defendant is accused of willfully failing to report as income nearly $1 million in cash that he brought back from a gambling trip to Macau. Defendant is likewise accused of willfully failing to report millions of dollars in gambling winnings from "heads up" poker matches elsewhere in Asia. The Indictment alleges that a Malaysian citizen, who had a relationship with a financial institution in Montenegro, assisted Defendant in those matches. Further, Defendant is accused of willfully failing to report income that was funneled by that Malaysian citizen through the Montenegrin financial institution where they both held accounts. Defendant's ties to gamblers and individuals in other countries, and his extensive international travel, mean that he is far better equipped than the average defendant to flee the United States to avoid the serious felony charges that he faces.

iii. Defendant's Concealment of his Cryptocurrency Transactions

Defendant's criminal conduct involved significant use of cryptocurrency, which he also concealed from the Government. Defendant is specifically charged with concealing millions of dollars in cryptocurrency transactions from the IRS. More particularly, Defendant "falsely stated on his 2020 and 2021 Forms 1040 that he had not received, sold, sent, exchanged, or otherwise acquired or disposed of any financial interest in any virtual currency—despite the fact that he had engaged in dozens of cryptocurrency transactions totaling over $10 million over those two tax years." ECF 1 at 10. During 2020, Defendant "maintained a United States-based cryptocurrency account" through which he engaged "in approximately 80 transactions involving the receipt, sale, sending, exchange, or acquisition of [cryptocurrency], with a total transaction volume of more than $1.5 million." ECF 1 at 27. During 2021, Defendant "maintained two cryptocurrency accounts, one in the United States and the other abroad." ECF 1 at 30. Through those accounts, Defendant "engaged in approximately 200 transactions . . . with a total transaction value of more than $8 million." ECF 1 at 30.

Moreover, Defendant was aware, since at least March 2020, that he was obligated to report cryptocurrency transactions to the IRS because his law firm's "then-firm manager reviewed with [Defendant] a tax organizer" from his accounting firm that included "a question . . . concerning whether he had engaged in cryptocurrency transactions." ECF 1 at 27. "Similarly, the Accounting Firm's retention letters in tax years 2019 and 2020 explicitly stated that cryptocurrency transactions needed to be reported on Forms 1040." ECF 1 at 27.

Defendant's efforts to engage in difficult-to-track cryptocurrency transactions are made plain by an analysis of the accounts he opened and used. More specifically, Defendant initially created a United States-based cryptocurrency account hosted at Coinbase in June 2020. But in

February 2021, Defendant created an account at Binance.com, a foreign-based cryptocurrency platform that prohibited U.S. residents from maintaining accounts. To create and maintain that account (despite the "U.S. resident" ban), Defendant appears to have used a virtual private network ("VPN") to make his device's location appear to be abroad, in places like Milan, Italy, and Oslo, Norway. Exhibit 1 (access log). During 2021, Defendant received cryptocurrency worth approximately $972,000 through his overseas Binance.com account and transferred approximately $660,000 in cryptocurrency from it to his domestic Coinbase account. Defendant overwhelmingly stopped using both accounts by the end of 2021.

iv. Defendant's Switch to Unhosted Cryptocurrency Wallets

In 2022, Defendant shifted from wallets hosted at exchanges—namely, Coinbase and Binance—to unhosted wallets not attributable through any exchange.

1. The 34DF Wallet

For example, on April 8, 2022, Defendant transferred 4,100 USDT to [redacted], a former romantic partner, from an unhosted wallet, [redacted]34df ("34DF wallet"). Exhibit 2. On May 11, 2022, Defendant transferred 3,000 USDT to [redacted] from the same 34DF wallet. *Id.* That 34DF wallet's most recent transaction occurred in December 2022 and, as of the time of the arguments before Judge Sullivan, still contained approximately $2,150 worth of cryptocurrency.[3]

2. The 0524 and B351 Wallets

In the past two years, Defendant has continued to fund and use unhosted wallets. For example, Defendant frequently enlisted the services of [redacted], who was the CEO of a

[3] The total amount of cryptocurrency in the 34DF wallet and B351 wallet (discussed below) have not changed since the February 13 hearing but the equivalent dollar value of that cryptocurrency has declined because of fluctuations in the cryptocurrency markets.

luxury travel and concierge service, and self-described "fixer" for ultrawealthy individuals (the "Fixer").[4] In July 2023, Defendant wired a total of $463,900 to the Fixer to purchase USDT cryptocurrency through three transactions for $106,900, $275,000, and $82,000 respectively, for which the Fixer invoiced Defendant. Exhibit 3. On July 21, 2023, Defendant provided the wallet address [redacted]b351 ("B351 wallet") to the Fixer, who then conducted a test transfer of 100 USDT that day.[5] Exhibit 4. On July 23, Defendant asked the Fixer if he had sent the remainder of the cryptocurrency and wrote, "If not, I have a new address." Defendant then provided the new address, [redacted]0524 ("0524 wallet"). *Id.* The Fixer then transferred $378,726 in USDT to the 0524 wallet. On August 12, 2023, the 0524 wallet transferred 369,000 USDT to the B351 wallet that Defendant had initially suggested to the Fixer. *Id.*; Exhibit 5.

On February 28, 2024, Defendant purchased a $13,500 luxury watch from [redacted] ("the Watch Dealer"), by transferring 13,500 USDT from the B351 wallet to the Watch Dealer's wallet, [redacted]Ea07e. Exhibit 6; Exhibit 7. Defendant described the watch as a present for another romantic partner of his, [redacted]. On March 22, 2024, Defendant purchased a $9,500 luxury watch from the Watch Dealer, sending 9,500 USDT from the B351 wallet to the Watch Dealer's same wallet. Exhibit 6; Exhibit 8. Defendant described the watch as a present for [redacted], another romantic partner of his. The B351

[4] Defendant asserts that the Government chose a pejorative term, "the Fixer" to cast suspicion on the Defendant's transactions with him. *See* ECF 81 at 3 n.3. The Government used this term because that is how [redacted] describes himself on his website. *See* [redacted]

[5] A minute after that transaction, Defendant texted the Fixer, "Waiting for [redacted] to land," referencing his then-romantic partner. The Fixer later texted, "I sent the $100. Was waiting for you to receive confirmation from [redacted]." This suggests [redacted] controlled the wallet or managed it on behalf of Defendant. However, as discussed below, Defendant's subsequent use of that to purchase watches for others strongly suggests that even if she managed the wallet, he controlled its use.

wallet conducted transactions worth hundreds of thousands of dollars in May and June 2024. It currently contains almost $15,000 worth of cryptocurrency.

Notably, Defendant does not dispute that he failed to disclose the 34DF and B351 wallets to Pretrial Services or the Court, although he now claims to "not currently control" them, ECF 81 at 24.

3. The 935B and 54E3 Wallets

It is also undisputed that, in 2023, Defendant caused large sums of cryptocurrency to be transferred to two other unhosted cryptocurrency wallets, the 935B wallet[6] and the 54E3wallet.[7] The timing of recent transactions to and from the wallets suggests that one or more of the transactions may have been done by or at the direction of Defendant. Regardless, the facts regarding these wallets are further examples of Defendant using cryptocurrency for his financial shell game.

For the 935B wallet, the chats between Defendant and the Fixer demonstrate Defendant's use of that wallet, which is further corroborated by Defendant's financial records and the transactions in the wallet. Specifically, on April 23, 2023, the Fixer messaged Defendant, "I am working on this deal for the Crypto transfer. He said he can do USDT or USDC. Would you mind sharing *your address* on where he would need to send each coin?" Exhibit 9 at 1 (emphasis added).[8] Defendant responds, "*I* can definitely take $500K crypto. But *I* have to structure it as a purchase. Like I have to have a record of buying it from him [someone going to Dubai with the Fixer]. Or from you. I need to do that bc *I'm* going to send it to Larry as his share of poker." *Id.* (emphasis added). While Defendant references using the cryptocurrency to pay Larry for his share

[6] The full address of the wallet is [redacted]935B.
[7] The full address of the wallet is [redacted]54E3.
[8] "USDT" and "USDC" are acronyms for two cryptocurrencies—"Tether" and "USD Coin," respectively.

of poker, nowhere in the chat does Defendant state that the funds will be sent directly to Larry and not to him. Indeed, minutes later, after the Fixer asked Defendant how he wanted to structure the transaction, Defendant replies, "I would have him send it to a wallet of yours. Then do an invoice to sell it to me. I'll wire you and have you send the coins for me." *Id.* When the Fixer asked how he should send the cryptocurrency, Defendant responded, "it doesn't matter so long as your accounting is sound. A lot of people would just buy a cold wallet." *Id.* The Fixer confirms that he has "a ledger one." *Id.* Therefore, from the start of the transaction, Defendant indicated that he was going to purchase the cryptocurrency and have it sent to him, and that at least the Fixer's transfer would take place using a cold, *i.e.* unhosted wallet.

Defendant and the Fixer then proceeded with the plan. The Fixer sent Defendant the requested invoice. *See id.* at 3; Exhibit 10 (invoice). Defendant then wired $500,000 to the Fixer. *See* Exhibit 9 at 3–4; Exhibit 11 at 1 (Defendant's wire transfer records); Exhibit 12 (Defendant's bank account statement). On May 1, 2023, the Fixer messages Defendant, "I have *your coin* in the wallet ready to go when you are." Ex. 1 at 4 (emphasis added). On May 5, 2023, Defendant asks what kind of cryptocurrency it is. *Id.* at 5. The Fixer responds that it is USDC and asks "which wallet to send to?" *Id.* Defendant then gives the address of the 935B wallet, confirms receipt of a test transfer, and then confirms receipt of the $500,000 that he purchased.

Three days after the 935B wallet received that $500,000 in USDC on May 5, 2023, the wallet sent that same amount to another wallet. Exhibit 13 (935B USDC transactions) at 1. This outflow reinforced the Government's inference—based on the evidence available when it sought detention—that Defendant received $500,000 in USDC to *his own wallet* (935B) and soon after then sent that amount from his wallet to one owned by Larry.

Defendant proffers evidence—not previously available to the Government—of parallel messages on an encrypted platform, WhatsApp, between Defendant, an unidentified number, and an individual identified as "Tiger." The name of the group chat is "poker player tom." Defendant submits that because Tiger sent Defendant the 935B wallet address on behalf of the unidentified number and confirmed receipt of the funds, Defendant does not own the 935B wallet. He also argues that because he was detained when the 935B wallet conducted a 2,000,000 USDT withdrawal on February 11, 2025, this also reinforces that he does not own the wallet. Finally, defendant also submits the expert declaration of Jason Trager, who submits, "In my experience, shared ownership of cryptocurrency wallets is strongly disfavored and very uncommon." ECF 81-1 ¶ 26.

But all this misses the point. First, Defendant has shown only that he needed someone else to provide the public address for the 935B wallet and that someone other than him accessed that wallet while he was detained.

Second and more importantly, even Defendant's own version of events reinforces his risk of flight. According to Defendant, he directed a third-party to send $500,000 in USDC to the unhosted 935B wallet, whose address was provided by "Tiger" at the behest of an unnamed individual he now dubs "the 818 number," ECF 81 at 13. According to his own expert, the 935B wallet has received and sent approximately $100,000,000 in cryptocurrency between its creation in November 2022 and the present. ECF 81-1 ¶¶ 31, 33. In other words, to pay Larry "his share of poker," Defendant funded a wallet that has had roughly $100 million in transactions. Even if Defendant does not own or control the 935B wallet, these facts show Defendant's connection to individuals—possibly abroad—who have controlled tens of millions of dollars in cryptocurrency through an unhosted wallet. And his use of the Fixer to route cryptocurrency through a third-party

to the 935B wallet further underscores how Defendant has used, and can continue to use, unhosted cryptocurrency wallets to facilitate transfers of large sums of money with gambling and/or foreign contacts.

The same is true for the 54E3 wallet. The 54E3 wallet was first used when Professional Gambler-1 transferred Defendant $242,410 in USDT on June 6, 2023, to pay Defendant for a poker loss. *See* Exhibit 14 (Professional Gamber-1 subpoena response letter). In other words, Defendant specifically used the 54E3 wallet to obtain a poker payment from Professional Gambler-1, with no indication that Professional Gambler-1 was paying someone else.

Defendant proffers that encrypted messages not previously available to the Government suggest that the payment was actually sent to an unidentified "Mr. T." In those messages, someone using an unidentified number asks Defendant whether he wants to pay Mr. T for a "debt due," and sends Defendant the 54E3 wallet number. Here again, even if Defendant does not own the 54E3 wallet, the transaction is yet another instance of how Defendant directed large sums of money to cryptocurrency to others—possibly gambling or foreign contacts—with obscured identities.

Moreover, the timing of recent transfers suggests that one or more of the transfers may have been done by or at the direction of Defendant. The 935B wallet was opened within two weeks of when Defendant stopped using his Coinbase account, which is also at a time Defendant knew he was under investigation. The 935B wallet was consistently used since that time with some transactions each month up to December 21, 2024. Exhibit 15 (935B USDT transactions) at 1-4. The transactions stopped until February 4, 2025—six days after Defendant's initial appearance and the day prior to Defendant's *pro se* motion—then there was an incoming transfer of $8 million USDT into the wallet followed by a $3 million transfer USDT out of the wallet. On February 6, 2025, at 11:41 PM EST—approximately *30 minutes* after the Government filed its

motion to strike Defendant's *pro se* motion—approximately $3 million more of USDT was sent out of the wallet, leaving approximately $2 million in the wallet. Defendant was arrested on February 10, 2025 and detained following a hearing on the Government's *ex parte* motion. ECF 41, 42. On February 11, 2025, while Defendant was detained, the remaining $2 million USDT left the wallet. While this suggests that Defendant was not the exclusive owner or user of the 935B wallet, it does not diminish the simple fact that Defendant had previously coordinated with gambling and possibly foreign contacts regarding transfers into the wallet and that the recent transactions directly coincided with Defendant's efforts to shed the bond condition on his Washington, D.C. residence.

The evidence regarding the 54E3 wallet is even clearer. As explained above, the 54E3 wallet was first used when Professional Gambler-1 transferred Defendant $242,410 in USDT on June 6, 2023 to pay Defendant for a poker loss. *See* Exhibit 14. The 54E3 wallet was dormant until, on February 5, 2025, at 4:10 AM EST—the day Defendant filed his *pro se* motion—the wallet received an incoming transfer of $1,306.32 in USDT. *See* Exhibit 16. One minute later, at 4:11 AM EST, a transfer of $22,006.84 in USDT went out of the wallet. *Id.* In other words, there were no transactions using the wallet from the day that Professional Gambler-1 used the wallet to pay Defendant for a poker loss until there were two the day that Defendant filed his *pro se* motion to shed the bond on his Washington, D.C. residence—a period of *one year, seven months, and thirty days*. To call this a coincidence is an understatement. Rather, it corroborates that the transfer of these funds was done by or at the direction of Defendant. At a minimum, it serves as yet another example of large sums of cryptocurrency being transferred to and from an unhosted wallet that Defendant has used to facilitate his financial subterfuge.

4. Unknown Wallets

In addition to Defendant's involvement with the above-described cryptocurrency wallets, there is evidence indicating that Defendant has recently used one or more other cryptocurrency wallets, which have not been disclosed to the Court or Pretrial Services.

For example, the Government understands that in July 2024, Defendant traveled to Mykonos, Greece to attend a multi-day birthday party. The party also was attended by other ultrahigh-stakes poker players. During the party, Defendant played in a series of poker matches with other attendees, and lost substantial sums of money. At one point, after Defendant had already lost a substantial sum of money, he paid approximately $200,000 in cryptocurrency to the "game runner" whose responsibility was to coordinate the process of settling wins and losses among the players. The Government is not aware of the identity of the cryptocurrency wallet that Defendant used to make the $200,000 payment, nor the identity of the owner of the cryptocurrency wallet (whether Defendant, a third party, or some combination). Regardless, this is another recent example of Defendant's access to and use of cryptocurrency. And even if Defendant was using someone else's cryptocurrency wallet to effectuate the transfer—such that he could argue he is not required to disclose the wallet to the Court and to Pretrial Services—it only underscores the importance of continuing to monitor Defendant's electronic devices to prevent him from using cryptocurrency transactions to attempt to flee or, as detailed next, to interfere with the investigation or potential witnesses to his criminal conduct.

v. Defendant's Attempt to Influence a Witness with Cryptocurrency

Defendant also has offered to pay a potential witness cryptocurrency, under circumstances that strongly suggest he sought to obstruct the investigation. The Government agrees with Defendant that this is a "very serious accusation," ECF 81 at 23—and it is borne out by the facts.

From 2019 through 2021, the potential witness was a "firm manager" at Defendant's law firm, Goldstein & Russell, P.C. ("G&R"). In that role, the potential witness was responsible for, among other things, recordkeeping, paying bills, employee health insurance, and working with an outside accounting firm on the law firm's and Defendant's taxes. The potential witness gained a unique understanding of the law firm's and Defendant's finances and income. The potential witness also learned that Defendant had "hired" a woman with whom he was in an intimate relationship, and caused her to be added to the law firm's health insurance plan, even though the woman did no work for the law firm.

The investigation into Defendant's tax misconduct went overt on October 14, 2020, when IRS Criminal Investigation ("IRS-CI") special agents visited Defendant's office to interview him and to request documents. The potential witness was at the law firm's office that day, working at the reception desk, and interacted briefly with the IRS-CI special agents. From the reception desk where the potential witness worked, she observed Defendant being interviewed by the IRS-CI special agents.

The very next day, the potential witness announced her resignation from the law firm, while making clear to Defendant and others at the law firm that she would remain in her position until a replacement was hired and trained. Soon after, Defendant told the potential witness that her resignation would look suspicious to the IRS and began offering her various things of value.

In early December 2020, G&R hired the potential witness's replacement. Her replacement then started work remotely at the firm on January 4, 2021, and then began working there in-person on January 18, 2021. During this time, the potential witness remained at G&R and trained her replacement.

Despite hiring and on-boarding the potential witness's replacement, Defendant escalated his offers to the potential witness. Even after her replacement was working in-person at the firm, Defendant offered the potential witness a $10,000 bonus, student loan payments, and cryptocurrency. Specifically, Defendant offered the potential witness Bitcoin,[9] and suggested that she download a mobile application that would enable such a transfer. Despite the fact that Defendant and the potential witness often communicated via text message and email, Defendant always approached her about cryptocurrency and Bitcoin in person. The potential witness told at least one associate in late January 2021 that Defendant's offers made her uncomfortable, and suggested that Defendant made the offers because he was concerned about the investigation into his taxes. These offers persisted through the potential witness's last day at the law firm in late January 2021.

To the Government's knowledge, Defendant never made similar offers to other departing G&R firm managers.

Against this backdrop, the Government reiterates that Defendant "had no credible reason to make the offers other than to attempt to prevent the potential witness from assisting in the investigation, or ensure that the potential witness would not divulge the full truth about Defendant's conduct." ECF 34 at 9. The evidence undermines Defendant's argument that his conduct in this regard was an "utterly commonplace" attempt to "induce[] [the potential witness] to remain with the firm." ECF 81 at 23-24. Indeed, as noted, Defendant's offers to the potential

[9] The exact amount of Bitcoin that Defendant offered the potential witness is unclear. That said, it bears noting that the value of a Bitcoin between October 2020 and January 2021 (a period during which Defendant repeatedly offered Bitcoin to the potential witness) ranged from approximately $11,000 (in mid-October 2020) to approximately $30,000 (in late-January 2021), with a high of approximately $40,000 (on January 9, 2021). Therefore, even if Defendant meant to offer the potential witness only one Bitcoin or even a fraction of a Bitcoin, the value of that offer could amount to a substantial percentage—and potentially more than half—of the potential witness's salary in 2020.

witness continued after it became obvious that she was not going to stay with the firm, after her replacement was hired, and even after her replacement began working there in-person. Defendant's use of cryptocurrency in this context further confirms the reasonableness of the Monitoring Condition.

vi. Defendant's Continued Concealment of Income

Beyond concealing his financial transactions from Probation and the Court, Defendant has continued his criminal nondisclosure of cryptocurrency transactions, and millions of dollars of income, to the IRS, in the most recent years for which tax returns were due. In particular, Defendant received over $12 million in net gambling winnings in 2022, yet failed to file a personal income tax return for that year with the IRS. Exhibit 17. Likewise, Defendant received over $10 million in gambling winnings[10] in 2023 but failed to file a tax return with the IRS for that year as well. *See* Exhibit 18 (payments a single player made to Defendant).

Defendant's willful failures to file tax returns for 2022 and 2023 not only served to deprive the Government of information concerning his tax liabilities for those years, they also served to further prevent the IRS from receiving an acknowledgment that Defendant, as in 2020 and 2021, had transacted in any virtual currency.[11] Given this additional conduct, which clearly constitutes crimes, Judge Sullivan was entirely justified in concluding that enhanced conditions of release were warranted.

[10] This reflects the gross gambling winnings Defendant received from just one player. Depending on staking arrangements, Defendant's personal gross winnings may be lower—but Defendant himself obscured the extent of his winnings by not filing a tax return.

[11] The law is clear that "[t]he pendency of a government investigation does not give a taxpayer a Fifth Amendment option to fail to file his tax return." *United States v. Josephberg*, 562 F.3d 478, 494 (2d Cir. 2009).

* * *

The foregoing transactions, spanning 2021 through 2024, demonstrate Defendant has routinely concealed his cryptocurrency activities by using an account based abroad and using unhosted wallets to conduct hundreds of thousands of dollars in transactions, in addition to offering cryptocurrency to a potential witness in this case and otherwise concealing his income from the Government. Therefore, the nature and circumstances of the offense strongly support the Monitoring Condition.

b. Weight of the Evidence

The powerful weight of the evidence also supports the Monitoring Condition. As the Government previously explained and the Court observed, the Indictment is supported by, among other things, "the Defendant's contemporaneous communications, documented loans that were not disclosed to mortgage lenders, bank and wire records, gambling-related memoranda authored by the Defendant, tax and accounting records, and records reflecting the Defendant's spending habits during the relevant period." ECF 76 at 6. The Government has collected and produced in discovery tens of thousands of documents proving his crimes, and the Government has identified nearly 80 witnesses whose testimony could also help prove the crimes. At trial, the Government will introduce this comprehensive and conclusive evidence.

Of particular relevance to the Monitoring Condition, the evidence is also strong with respect to Defendant's use and concealment of cryptocurrency. As explained above, Defendant is charged with falsely stating on his 2020 and 2021 tax returns that he did not engage in any cryptocurrency transactions, when in reality Defendant engaged in dozens of cryptocurrency transactions totaling over $10 million over those two tax years. The evidence here is irrefutable, because Defendant conducted these transactions in cryptocurrency accounts that he made in his

own name (despite efforts at obfuscation by using a foreign Binance account while in the United States), before switching his cryptocurrency accounts to unhosted wallets which are much more difficult for the government to identify.

The evidence is also strong regarding Defendant's continued use of unhosted cryptocurrency wallets. Defendant principally argues that he does not own or control the 935b and 54E3 wallets. *See* ECF 81 at 10–22. As explained above, however, the timing of the recent transactions in these accounts strongly suggests Defendant's involvement. Either way, it is undisputed that, at the very least, Defendant diverted payments from third parties to these accounts. It is also undisputed that Defendant conducted transactions using the 34DF, 0524, and B351 wallets, and that Defendant failed to disclose these to Pretrial Services and the Court. Further, it is undisputed that Defendant has continued to conceal his assets, including millions of dollars in gambling income, by failing to file tax returns since tax year 2021.

Thus, the weight of the evidence concerning Defendant's use and concealment of cryptocurrency supports the Monitoring Condition.

c. History and Characteristics of Defendant

As the Court previously found, "The Defendant's personal history and characteristics also indicate that he is a significant flight risk." ECF 76 at 6. The Court correctly observed that the Defendant has extensive experience with international travel and significant ties to wealthy individuals in foreign countries that could make it easier for him to flee than the average person. *Id.* "Those concerns heighten the Defendant's risk of flight here." *Id. See also United States v. Remarque*, PX-19-039, 2020 WL 1983927, at *1-*4 (D. Md. Apr. 27, 2020) (denying appeal of Judge Sullivan's pretrial detention order based on, among other things, defendant's "significant international ties"); *United States v. Fombe*, DKC-19-452-1, 2023 WL 6200018, at *2 (D. Md.

Sept. 22, 2023) (denying motion for review of Judge Sullivan's pretrial detention order because, among other reasons, defendant had overseas contacts and had demonstrated "the wherewithal to flee, using false documentation, and to travel to myriad foreign countries"); *United States v. Raji*, SAG-20-00369, 2021 WL 825981, at *1-*2 (D. Md. Mar. 4, 2021) (denying motion to reconsider pretrial detention where defendant had the "'motive, means and contacts' to flee and assume another identity either in the United States or abroad"); *United States v. Anderson*, 384 F. Supp. 2d 32, 36 (D.D.C. 2005) (finding a defendant's history and characteristics in a tax evasion case weighed in favor of detention based on the defendant's "substantial assets abroad; his connections overseas; . . . his lack of ties to the District of Columbia; and his persistent deceitfulness . . . in his dealings with the government").

These concerns regarding Defendant's risk of flight are directly relevant to Defendant's use and concealment of cryptocurrency and the appropriateness of the Monitoring Condition. Defendant routinely conducted cryptocurrency transactions with foreign gambling contacts and individuals located abroad. And as described above, it appears that Defendant specifically used a foreign-based Binance.com account by circumventing restrictions on U.S. residents by creating and maintaining a VPN to access that account, before switching to unhosted wallets with no restrictions at all. As discussed in Section II below, it is exactly this type of concealment and use of cryptocurrency that could facilitate Defendant's flight and ability to leverage his foreign contacts, supporting the appropriateness of the Monitoring Condition.

d. Danger to Community

Defendant remains an economic danger to the community. As alleged in the Indictment, Defendant owes millions of dollars in unpaid taxes to the federal government and to private individuals. Should Defendant flee, or continue to conceal assets held in cryptocurrency wallets

and cryptocurrency transactions, both the public and Defendant's private creditors would be substantially harmed. *See United States v. White*, PWG-13-0436, 2015 WL 2374229, at *2 (D. Md. May 15, 2015) ("[E]conomic danger may qualify as a basis for detention under 18 U.S.C. § 3148." (citing *United States v. Gill,* 2008 WL 2120069, at *3 (E.D. Cal. May 20, 2008) (quoting *United States v. Reynolds,* 956 F.2d 192–93 (9th Cir.1992) (ruling in a violation of pretrial release hearing that "danger may, at least in some cases, encompass pecuniary or economic harm"))); *United States v. Madoff,* 586 F. Supp. 2d 240, 253 (S.D.N.Y.2009) ("The Court recognizes . . . that there is jurisprudence to support the consideration of economic harm in the context of detention to protect the safety of the community").

In addition, as described above, the evidence indicates that Defendant offered things of value, including cryptocurrency, to a potential witness in the case who had intimate knowledge of his and his law firm's finances and income—and that there was no other credible reason for doing so than to attempt to prevent the potential witness from assisting in the investigation. This raises the serious concern that Defendant could use cryptocurrency to attempt to influence other witnesses in this case. Such conduct would be harmful to the administration of justice, to the integrity of this Court, and to the integrity of the court system more broadly.

Therefore, Defendant's economic danger to the community weighs in favor of the Monitoring Condition.

II. The Monitoring Condition is Appropriate under the Bail Reform Act

The Bail Reform Act requires that the Court impose on the defendant "the least restrictive" condition(s) of pretrial release that the Court determines "will reasonably assure the appearance of the [defendant]." 18 U.S.C. § 3142(c)(1)(B). The Bail Reform Act enumerates thirteen available

standard conditions and also allows the Court to impose "any other condition that is reasonably necessary to assure the appearance of the [defendant]." *Id.* § 3142(c)(1)(B)(xiv).

In light of the Bail Reform Act factors discussed above, the instant Monitoring Condition—that Defendant's electronic devices be monitored by Pretrial Services—is necessary as part of the least restrictive combination of conditions of pretrial release that will reasonably assure Defendant's appearance. Indeed, it is far less restrictive than the pretrial detention courts often find necessary to assure the appearance of defendants with significant cryptocurrency activity.

In *United States v. Sterlingov*, 573 F. Supp. 3d 28 (D.D.C. 2021), the defendant was charged with money laundering and related crimes for operating an illegal service that helped users launder illicitly acquired cryptocurrency. *See id.* at 30-31. After the magistrate judge ordered him detained based on a serious risk of flight, Sterlingov moved to revoke pretrial detention, requesting that he instead be "release[d] on home detention [with] location monitoring and internet restrictions" *Id.* at 30, 33–34. The government alleged that Sterlingov had made "at least $8 million . . . in cryptocurrency proceeds." *Id.* at 38. In examining the defendant's history and characteristics, the court acknowledged that "the government lacks any admissions or direct evidence of his assets," but Sterlingov was accused of operating a service "to conceal financial transactions," and "[t]he prospect that the government has not located all of [his] assets, particularly his cryptocurrency accounts, is thus unsurprising." *Id.* The court noted that the government identified "over $800,000 in U.S. dollars and cryptocurrency" after Sterlingov submitted a financial disclosure form that failed to report these assets, and further noted the evidence suggested he was adept at disguising his funds' origins. *Id.*

The court concluded that Sterlingov likely "ha[d] additional funds that the government ha[d] yet to identify, which could be available to fund an effort to flee the country." *Id.* at 39.

Further, Sterlingov's history of obfuscating his online activity meant pretrial services could not adequately monitor his activity. *Id.* In light of his history and characteristics, as well as the other § 3142 factors, the court held that no combination of conditions could reasonably assure the defendant's appearance. *Id.* at 40.

Similarly, in *United States v. Dawodu*, No. CR 21-163 (JDB), 2022 WL 1556403 (D.D.C. May 17, 2022), the relevant defendant, Alex Ogando, sold opioids online in exchange for cryptocurrency and was ordered detained before trial. *See id.* at *1. He moved to revoke the detention order but the court upheld detention, concluding that no combination of conditions could mitigate the risks of flight and harm to the community. *See id.* at *7-8. On the former risk, the court noted that Ogando had "apparent access to funds, including difficult-to-trace cryptocurrencies, would make flight from prosecution easier," as would his ability to use the darknet to acquire materials that would help him flee. *Id.*

The Bail Reform Act factors discussed above demonstrate that Defendant poses much the same risk of flight as the defendants in *Sterlingov* and *Dawodu*. Defendant has proven adept at concealing his assets through cryptocurrency. As described above, he used his overseas account hosted at Binance.com to conceal his receipt of nearly $1 million in cryptocurrency and to hide nearly $300,000 of that by using Binance.com, a company outside the jurisdiction of the United States. Moreover, he appears to have done so through a VPN, effectively hiding his conduct and Binance.com account from anyone—including the Government—that might have tried to identify it based on his internet use.

Defendant then used unhosted wallets to continue transacting in cryptocurrency as recently as last year. As Defendant's expert recognizes, "an unhosted wallet provides a user complete control over cryptocurrency" and "complete ownership" of the contents of the unhosted wallet.

Appeal Ex. A ¶ 25, ECF 80-1 (Jason Trager Expert Decl.). But that expert artfully avoids acknowledging the other key—and deeply troubling—aspect of unhosted wallets: although the transactions of an unhosted wallet are public, the *identity* of its owner is hidden because the owner maintains all control of the wallet. There is no exchange (like Coinbase) that can be subpoenaed. The Government cannot directly identify which or how many unhosted wallets a person owns. Instead, a particular unhosted wallet can be attributed to a particular owner only if the owner reveals his or her ownership to another party (who then provides that information to the government), or the government seizes a device or document that effectively identifies the owner. This means that the Court cannot confirm or disprove Defendant's claim that he does not currently control any cryptocurrency through unhosted wallets.

In short, Defendant used an overseas Binance.com account through a VPN, and then controlled multiple unhosted wallets, conducting transactions as recently as last year. Notably, Defendant *does not contest* these facts on appeal.

Moreover, through the few accounts that the government *has* been able to attribute to Defendant, he has conducted millions of dollars in cryptocurrency transactions. Defendant's history of obscuring his cryptocurrency through a foreign-based exchange and unhosted wallets presents precisely the concern in *Sterlingov*: Defendant's sophisticated efforts to conceal his financial transactions make it "unsurprising" that the government may not have located all his "assets, particularly his cryptocurrency accounts," and likely that he "has additional funds the government has yet to identify, which could be available to fund an effort the flee the country," *Sterlingov*, 573 F. Supp. at 38; *see also Dawodu*, 2022 WL 1556403, at *7 ("[Defendant's] apparent access to funds, including difficult-to-trace cryptocurrencies, would make flight from prosecution easier . . . .").

This is precisely the concern that Judge Sullivan stated when imposing the Monitoring Condition and others: "These added restrictions are necessary to reasonably assure that Mr. Goldstein appears as required. Given Mr. Goldstein's extensive past use of cryptocurrency, the Court finds it likely that Mr. Goldstein has access to funds that have yet to be identified, and which he might use to flee from prosecution in this case." Det. Mem. 6, ECF 64.

Defendant's apparent experience obscuring his internet activity through a VPN only heightens this concern, as does his long history of using encrypted messaging platforms, such as WhatsApp, and encrypted email platforms based abroad. *Cf. Dawodu*, 2022 WL 1556403, at *7 (noting defendant's "expertise with technologies—including encrypted messaging, cryptocurrencies, and the darknet—can hinder law enforcement's ability to detect illegal activity").

a. Defendant failed to disclose his ownership and now obfuscates his connection to known wallets.

As the Indictment alleges, Defendant repeatedly failed to report his cryptocurrency transactions to the IRS. More recently, he failed to disclose any cryptocurrency assets to Pretrial Services in his original financial disclosures. These include the unhosted 34DF wallet, which last transacted in December 2022 and still contains roughly $2,150 in cryptocurrency, and the unhosted B351 wallet, which conducted hundreds of thousands of dollars in transactions in May and June 2024, and currently contains almost $15,000 in cryptocurrency.

Defendant now concedes that he previously controlled these wallets but claims that he "no longer has access to [the unhosted 34DF and B351] wallets," and "does not currently control these accounts."[12] ECF 81 at 10, 22. These statements raise more questions than answers. Defendant has not explained how he lost control of those wallets, who now controls them, why they still

[12] The Government has not received information from Pretrial Services about Defendant's current cryptocurrency holdings.

contain large sums of cryptocurrency, or what—aside from his own volition—prevents him from regaining control of them. Nor does his filing offer any evidence to corroborate his claims.

Moreover, Defendant's failure to initially disclose these wallets—despite recently controlling them—raises the specter that he may have additional cryptocurrency assets that he still has not disclosed to the Court. *See Sterlingov*, 573 F. Supp. at 38 (noting defendant's failure to disclose cryptocurrency assets in his financial disclosure to the court); *United States v. Wang*, 670 F. Supp. 3d 57, 70 (S.D.N.Y. 2023) (noting defendant "ha[d] not been forthcoming in fully disclosing her assets," including "cryptocurrency redemption rights," and although there was "not proof [defendant] actually received or currently owns any cryptocurrency," the court remained concerned that the defendant had undisclosed assets and posed a serious risk of flight), *aff'd*, No. 23 CR. 118-3, 2023 WL 4551637 (S.D.N.Y. July 14, 2023). His July 2024 use of cryptocurrency to pay a multi-hundred thousand dollar bet—through accounts or third-parties yet unidentified—further underscores this risk.

In effect, Defendant now asks the Court to just trust him. But the Indictment alleges Defendant lied to the IRS, his accountants, his investors, and multiple mortgage lenders—all of whom initially trusted him. *E.g.*, ECF 1 ¶¶ 32-33, 36, 38, 43-45, 47, 89-92, 97-100. The Court should not make the same mistake.

b. The Monitoring Condition is the least restrictive condition that will reasonably assure Defendant's appearance.

The foregoing facts and precedent reinforce the high risk that Defendant has undisclosed cryptocurrency assets and—without adequate conditions of release—poses a significant risk of flight. Indeed, as Judge Sullivan noted, defendants in similar circumstances are typically *detained* because courts conclude that no combination of conditions of pretrial release can reasonably assure their appearance. *See* ECF 73 at 35 (noting that cryptocurrency-related defendants were

overwhelmingly detained in D.D.C. and S.D.N.Y. cases); *see, e.g.*, *Sterlingov*, 573 F. Supp. 3d at 40; *Dawodu*, 2022 WL 1556403, at *7; *Wang*, 670 F. Supp. 3d at 72; *see also United States v. Texeira-Spencer*, No. CR 21-145 (JDB), 2021 WL 1535309, at *8 (D.D.C. Apr. 19, 2021).

Defendant's long history of lying to others and obfuscating his cryptocurrency make it reasonably necessary to ensure he does not attempt to access or transfer undisclosed cryptocurrency in order to flee.

Monitoring his electronic devices is the least restrictive condition that will assure his appearance. Other options—such as detaining him or completely barring him from accessing the internet—are far more restrictive. Courts have frequently rejected even these more restrictive conditions as insufficient. *See, e.g.*, *Sterlingov*, 573 F. Supp. 3d at 30, 40 (affirming pretrial detention and declining defendant's proposal to release him on home detention with location and internet monitoring); *Dawodu*, 2022 WL 1556403, at *7 (affirming pretrial detention after concluding location monitoring and a ban on internet access would not suffice).

Defendant asserts that the conditions requiring him to disclose his cryptocurrency and prohibiting him from opening new financial accounts or using cryptocurrency will suffice. Appeal at 25. But the Monitoring Condition is necessary precisely because, without it, Pretrial Services and the Court will have no way to know whether Defendant his disclosed all his cryptocurrency or refrained from conducting cryptocurrency transactions.

Finally, the Monitoring Condition is also the least restrictive, reasonably necessary condition of pretrial release with respect to attorney-client privilege. First, electronic device monitoring is such a common condition that it is a *standard option* on the District of Maryland Conditions of Release Order form. *E.g.*, Order Setting Conditions of Release, ECF 6 at 3 (listing electronic device monitoring option in Additional Conditions of Release ¶ 8(v)); Am. Order

Setting Conditions of Release (same). Defendant does not argue that this condition is a facial violation of his rights, nor can he given its widespread use.

Second, the Monitoring Condition does not create a significant risk of the disclosure of attorney-client privileged information to the Government because Pretrial Services—an extension of the Court, not the Government—monitors the devices. Moreover, Pretrial Services does not manually review every communication and reports only apparent violations of the conditions. Rather, as the Court and Pretrial Officer Smith explained during the February 13, 2025 hearing, the Monitoring Condition simply permits a periodic review to ensure that Defendant is not engaging in cryptocurrency transactions:

> **MR. SMITH:** Your Honor, from my experience the monitoring equipment is just I review it monthly and it shows me what activity he's conducting. It shows me what, if any, applications he attempts to get onto. It's merely just an added layer of monitoring software that's in place in all of his –
>
> **THE COURT:** But you are not -- you have no ability or desire as pretrial to look at the contents of his emails or attachments that he receives or Word documents that he's preparing or for that matter, you know, what -- if he's going on the internet to the law firm to look at discovery, that's not a problem, is it?
>
> **MR. SMITH:** No. We have other pretrial defendants who have similar equipment placed on their computers, their internet-capable devices and, no, that's not what we're looking at.

ECF 73 (Tr. of February 13, 2025 hearing) at 40–41. Thus, there is no legitimate concern that the Monitoring Condition will cause privileged communications to be disclosed to the Government. Defendant's related claim that the condition threatens his "ability to provide legal advice to others by risking the disclosure of privileged communications," ECF 81 at 25, also fails for these reasons.[13]

[13] It is unclear whether Defendant is even working as an attorney. Defendant previously told Pretrial Services that he was no longer planning to pursue any legal consulting work.

Third, the Monitoring Condition restricts Defendant's attorney-client privileged communications far less than the alternatives. Completely barring him from internet access would even more severely limit those communications by precluding email or similar electronic communication. Barring all access to electronic devices would not only preclude such correspondence but also prevent him from digitally reviewing evidence for his defense or his clients. And detention would be far more restrictive.

Defendant's history of concealing his cryptocurrency through sophisticated means—including a VPN, a wallet hosted overseas, and multiple unhosted wallets—make him a significant risk of flight and make necessary conditions of pretrial release that will ensure the Court can know if he attempts to access or use undisclosed cryptocurrency. The Monitoring Condition is the least restrictive condition and is reasonably necessary to assure defendant's appearance.

CONCLUSION

For all the reasons stated above, the Government respectfully requests that the Court deny Defendant's appeal of the Monitoring Condition.

Respectfully submitted,

Kelly O. Hayes
United States Attorney
/s/
Patrick D. Kibbe
Assistant United States Attorney
District of Maryland

Stanley J. Okula, Jr.
Senior Litigation Counsel
Department of Justice—Tax Division

Emerson Gordon-Marvin
Hayter Whitman
Trial Attorneys
Department of Justice—Tax Division